APPENDIX A
CRS Password Modification Procedures & Lost Root User Password Recovery

This Appendix is taken from CRS EQUIPMENT MAINTENANCE NOTE 58. It provides CRS password modification procedures in compliance with Department of Commerce policies. The CRS password modification procedures must be performed Quarterly on all CRS Front End, Main, Voice Improvement Processors (FEPs, MPs, and VIP) as directed by CRS Password Change Day Policy (see page A-11).

General
These procedures detail which CRS user account passwords will be changed and how to change them.

CAUTION

Do not use special characters in any of the CRS user account passwords. Even though the Department of Commerce password management policy specifies the use of at least one number or special character in the password, the CRS application software currently will not allow the use of special characters. The use of a special character in any password will cause the GUI login attempt to fail. Therefore, until this problem is fixed, sites must use at least one number in all CRS passwords.

NOTE:

1. The CRS system must be running in a normal configuration, ie. 0MP as the Master MP and 5MP as the Shadow MP. All FEP's must be running in a normal configuration, ie. 4BKUP should not be an active FEP. The CRS and VIP applications must be stopped.
2. The following CRS user accounts are present on all CRS nodes: root, crs, **admin**, **maint** and **oper**.
3. The **switchmp** user account is only required on the 0MP and 5MP nodes. The **sysadm** user account is only required on the FEP nodes.
4. When changing system passwords, make sure the changes are made on each system node, i.e., 0MP, 5MP, 1FEP, 4BKUP and any remaining FEP nodes. The VIP has only user accounts **root** and **crs** that must be changed. Additionally, the LAN Server root user password must be changed.
5. The LAN server (ps8) root password is limited to a maximum of 8 characters. Therefore, if sites choose to have their root passwords match on all processors, they must limit them to 8 characters.

NOTE: 6. Passwords for all users must be changed at the same time. The warning and expiration messages will only be seen for those users that you log into. For example, most sites do not log in as crs user. Therefore, if the crs user password is getting close to expiration or has in fact expired, the operator may not see the warning or expiration messages. Therefore, sites must ensure that when they see the password warning or expiration message for one user, they change passwords for all users.

A-1 Preliminary System Setup Procedures

1. Before proceeding, read the entire procedure.
2. Schedule CRS downtime to perform this procedure. As a conservative estimate, schedule one hour to perform the procedure. This is a conservative estimate. The actual downtime may be less, or it may be more if you encounter problems.
3. Notify the public that CRS (NOAA Weather Radio) will be down during this scheduled time for maintenance.

NOTE: Please observer the following rules when defining good passwords:

1. A minimum of eight non-blank characters.
2. A minimum of one lower case alphabetic character in the first 8 characters.
3. A minimum of one upper case alphabetic character in the first 8 characters.
4. A minimum of one number in the first 8 characters.
5. Six of the characters may occur only once in the password.
6. Password must be changed at least every 90 days.
7. Password must not be used in the last 11 password changes.
8. Password cannot contain default passwords or words in dictionary.
9. **No special characters are allowed.**

A-2 Procedure for Changing VIP Passwords After They Have Expired

If a VIP user password expires, the user **will not** be prompted automatically to change the password. The user must perform the following steps to change the expired password:

1. Press **`CTRL-ALT-F1`** together to force a Linux login prompt.
2. Login as the user with the expired password. Follow the system prompts to change the password.
3. Press **`CTRL-ALT-F7`** together to return to the GUI screen.

A-3 Procedure for Changing Root and CRS User Passwords on the VIP

Check to see if the CRS application is running. If it is, stop the CRS application by clicking the **System menu** and then select **Stop System** and select **OK**. Wait until the application is stopped completely. Check to see if the VIP server is running. If it is, then stop the VIP server by clicking **Stop** on the **VIP main menu**. Then proceed with the following steps.

1. On the VIP, Click on **terminal** (lower left area of the screen) to open a Linux shell window.
2. Type:

   su

3. Enter the root password.

   password:[type in root password]

4. Type:

   passwd root

   Follow the prompts to change the root password

5. Exit the root user by typing:

   exit

6. Type:

   passwd

   Follow the prompts to change the crs password.

NOTE: 1. Use the same crs password used in the MPs and FEPs.

7. Exit the Linux shell by typing **exit**.

A-4 Procedure for Changing Passwords on the MPs and FEPs

1. On **0MP** open a **UNIX shell** window from the **Maintenance** menu.
2. Log in as the **root** user:

   0MP{admin} su

   Enter the **root** password.

   password:[type in root password]

3. Use the UNIX passwd command to change the user passwords on the 0MP

node. For the exact syntax and usage of the command, use the man passwd command string.

 # passwd root

Follow the prompts to change the password.

NOTE: 1. User switchmp password change cannot use the **passwd** command from the switchmp user. If this is done, it will force CRS to do an MP switch. The switchmp password must be changed using the **passwd switchmp** command from the root user.

 # passwd switchmp

Follow the prompts to change the password.

 # su - crs and enter the crs password if prompted.

0MP{crs} passwd

Follow the prompts to change the password.

0MP{crs} exit

 # su - admin and enter the admin password if prompted.

0MP{admin} passwd

Follow the prompts to change the password.

0MP{admin} exit

 # su - maint and enter the maint password if prompted.

0MP{maint} passwd

Follow the prompts to change the password.

0MP{maint} exit

 # su - oper and enter the oper password if prompted.

0MP{oper} passwd

Follow the prompts to change the password.

0MP{oper} exit

4. Exit the root user.

 # exit

5. Log into the **5MP** node using the **rsh** command:

0MP{admin} rsh 5MP

Log in as the **root** user:

5MP{admin} su

Enter the **root** password.

password:[type in root password]

6. Use the UNIX **passwd** command to change the user passwords on the 5MP node. For the exact syntax and usage of the command, use the **man passwd** command string.

NOTE: 2. The passwords should be changed to match the **0MP** node passwords.

 # passwd root

Follow the prompts to change the password.

NOTE: 3. User switchmp password change cannot use the **passwd** command from the switchmp user. If this is done, it will force CRS to do an MP switch. The switchmp password must be changed using the **passwd switchmp** command from the root user.

 # passwd switchmp

Follow the prompts to change the password.

 # su - crs and enter the crs password if prompted.

5MP{crs} passwd

Follow the prompts to change the password.

5MP{crs} exit

 # su - admin and enter the admin password if prompted.

5MP{admin} passwd

Follow the prompts to change the password.

5MP{admin} exit

 # su - maint and enter the maint password if prompted.

5MP{maint} passwd

Follow the prompts to change the password.

```
5MP{maint} exit
```

```
# su - oper
```
and enter the oper password if prompted.

```
5MP{oper} passwd
```

Follow the prompts to change the password.

```
5MP{oper} exit
```

7. Exit the **root** user and the **5MP** node by typing **exit** twice.

   ```
   # exit
   ```

   ```
   5MP{admin} exit
   ```

8. Log into the **1FEP** node using the **rsh** command:

   ```
   0MP{admin} rsh 1FEP
   ```

   Log in as the **root** user:

   ```
   $ su -
   ```

   Enter the **root** password.

   password:[type in root password]

9. Use the UNIX **passwd** command to change the user passwords on the **1FEP** node. For the exact syntax and usage of the command, use the **man passwd** command string.

NOTE:

4. The passwords should be changed to match the **0MP** node passwords where they exist. The **sysadm** password, which only exists on the FEPs, should be the same on all FEPs.

   ```
   1FEP{root} passwd root
   ```

   Follow the prompts to change the password.

NOTE:

5. You cannot switch remotely to the sysadm user because of terminal emulator problems. Therefore, the sysadm password must be changed using the **passwd sysadm** command from the root user.

   ```
   1FEP{root} passwd sysadm
   ```

   Follow the prompts to change the password.

1FEP{root} su - crs and enter the crs password if prompted.

$ passwd

Follow the prompts to change the password.

$ exit

1FEP{root} su - admin and enter the admin password if prompted.

$ passwd

Follow the prompts to change the password.

$ exit

1FEP{root} su - maint and enter the maint password if prompted.

$ passwd

Follow the prompts to change the password.

$ exit

1FEP{root} su - oper and enter the oper password if prompted.

$ passwd

Follow the prompts to change the password.

$ exit

1FEP{root} exit To exit the root password.

10. Exit the **1FEP** node by typing **exit**.

$ exit

Log into the **4BKUP** node using the **rsh** command:

0MP{admin} rsh 4BKUP

Log in as the **root** user:

$ su -

Enter the **root** password.

password:[type in root password]

11. Use the UNIX **passwd** command to change the user passwords on the **4BKUP** node. For the exact syntax and usage of the command, use the **man passwd** command string.

NOTE: 6. The passwords should be changed to match the **0MP** node passwords where they exist. The **sysadm** password, which only exists on the FEPs, should be the same on all FEPs.

4BKUP{root} passwd root

Follow the prompts to change the password.

NOTE: 7. You cannot switch remotely to the sysadm user because of terminal emulator problems. Therefore, the sysadm password must be changed using the **passwd sysadm** command from the root user.

4BKUP{root} passwd sysadm

Follow the prompts to change the password.

4BKUP{root} su - crs and enter the crs password if prompted.

$ passwd

Follow the prompts to change the password.

$ exit

4BKUP{root} su - admin and enter the admin password if prompted.

$ passwd

Follow the prompts to change the password.

$ exit

4BKUP{root} su - maint and enter the maint password if prompted.

$ passwd

Follow the prompts to change the password.

$ exit

4BKUP{root} su - oper and enter the oper password if prompted.

$ passwd

Follow the prompts to change the password.

$ exit

4BKUP{root} exit To exit the root password.

12. Exit the **4BKUP** node by typing **exit**.

    $ exit

NOTE: 8. Sites with more than two FEP nodes should change passwords on the remaining FEPs as applicable. See the following steps.

13. Log into the **2FEP** node using the **rsh** command:

    0MP{admin} rsh 2FEP

    Log in as the **root** user:

    $ su -

    Enter the **root** password.

    password:[type in root password]

14. Use the UNIX **passwd** command to change the user passwords on the **2FEP** node. For the exact syntax and usage of the command, use the **man passwd** command string.

NOTE: 9. The passwords should be changed to match the **0MP** node passwords where they exist. The **sysadm** password, which only exists on the FEPs, should be the same on all FEPs.

2FEP{root} passwd root

Follow the prompts to change the password.

NOTE: 10. You cannot switch remotely to the sysadm user because of terminal emulator problems. Therefore, the sysadm password must be changed using the **passwd sysadm** command from the root user.

2FEP{root} passwd sysadm

Follow the prompts to change the password.

2FEP{root} su - crs and enter the crs password if prompted.

$ passwd

Follow the prompts to change the password.

$ exit

2FEP{root} su - admin and enter the admin password if prompted.

$ passwd

Follow the prompts to change the password.

$ exit

2FEP{root} su - maint and enter the maint password if prompted.

$ passwd

Follow the prompts to change the password.

$ exit

2FEP{root} su - oper and enter the oper password if prompted.

$ passwd

Follow the prompts to change the password.

$ exit

2FEP{root} exit To exit the root password.

15. Exit the **2FEP** node by typing **exit**.

$ exit

16. Log into the **3FEP** node using the **rsh** command:

0MP{admin} rsh 3FEP

Log in as the **root** user:

$ su -

Enter the **root** password.

password:[type in root password]

17. Use the UNIX **passwd** command to change the user passwords on the **3FEP** node. For the exact syntax and usage of the command, use the **man passwd** command string.

NOTE: 11. The passwords should be changed to match the **0MP** node passwords where they exist. The **sysadm** password, which only exists on the FEPs, should be the same on all FEPs.

3FEP{root} passwd root

NOTE: 12. You cannot switch remotely to the sysadm user because of terminal emulator problems. Therefore, the sysadm password must be changed using the **passwd sysadm** command from the root user.

3FEP{root} passwd sysadm

Follow the prompts to change the password.

3FEP{root} su - crs and enter the crs password if prompted.

$ passwd

Follow the prompts to change the password.

$ exit

3FEP{root} su - admin and enter the admin password if prompted.

$ passwd

Follow the prompts to change the password.

$ exit

3FEP{root} su - maint and enter the maint password if prompted.

$ passwd

Follow the prompts to change the password.

$ exit

3FEP{root} su - oper and enter the oper password if prompted.

$ passwd

Follow the prompts to change the password.

$ exit

3FEP{root} exit To exit the root password.

18. Exit the **3FEP** node by typing **exit**.

    $ exit

19. Exit the **UNIX shell** window by typing **exit**.

    0MP{admin} exit

A-5 Procedure for Changing the LAN Server (ps8) Password

NOTE: 1. The CRS and VIP application software should not be running. If CRS application software is running, then stop the CRS application by clicking the System menu, selecting Stop System, and then selecting OK. Wait until the application completely stops. If the VIP application is running, stop the VIP application by clicking Stop on the VIP main interface menu.

1. Open a **UNIX shell** window from the **Maintenance** menu.

2. Type:

   telnet ps8

3. Log in as **root** user (default password is “dbps”)

4. Type:

   newpass

5. The system prompts:

   current password: [enter current password]

6. The system prompts:

   new password: [enter new password]

NOTE: 2. No more than 8 characters are allowed in the password.

7. The system prompts:

   repeat new password: [re-enter new password]

8. Type:

   exit

9. Start the CRS application software by clicking the **System menu**, selecting **StartSystem**, and then selecting **OK.** Start the VIP application by clicking **Start** on theVIP main interface menu.

A-6 Procedure for Changing the CRS User Password in the /data/fxa/workFile/nwr/nwr.cfg File on the AWIPS DS1 Node

AWIPS System Assumptions

The **/data/fxa/workFiles/nwr/nwr.cfg** file has been correctly configured on the site DS1 node. The file should contain, in strict order, the following information: CRS user name, password, and the interface type LAN. The CRS user password must be changed to match that used in CRS.

See the following example:

ds1-nmtw{awipsusr}2: cat /data/fxa/workFiles/nwr/nwr.cfg crs

XXXXX [Verify the correct crs user password here] LAN

ds1-nmtw{awipsusr}3:

NOTE: **Based on your system configuration**, change your CRS password on every AWIPS node where the nwr.cfg file exists. For example, if you run transferNWR on workstations to ftp messages to CRS, the CRS password must be changed there as well. If you are unsure of your specific configuration, please check with the AWIPS focal point.

A-7 Lost Root User Password Recovery

This procedure allows you to recover from a lost root user password scenario. To perform this procedure, the site must have previously created two sets of Emergency recovery diskettes (FEP and MP) in accordance with Chapter 5, "Creation of (FEP and MP) Emergency Recovery Diskettes."

NOTE: The CRS must be in a normal operating condition (i.e., 0MP as the Master MP and 5MP as the Shadow MP). All FEPs must be running in a normal configuration (i.e., 4BKUP should not be an active FEP).

To recover a lost 'root' user password:

1. Stop the CRS application software using the *XCRS_SITE* utility **Stop CRS System** menu selection.
2. **Boot** the MP or FEP machine using the appropriate Emergency Recovery Diskettes.
3. Select **Unmount File Systems** and press **<Enter>**.
4. Select **Mount File Systems** and press **<Enter>**.
5. Select **Access UNIXWare Shell** and press **<Enter>**.
6. At the 'root' prompt, type the following command and press **<Enter>**.

   #chroot /mnt passwd root
7. Enter the NEW root ***password*** and press **<Enter>**.
8. Re-enter the NEW root ***password*** and press **<Enter>**.
9. At the "root" prompt, type **exit** and press **<Enter>**.
10. Select **Reboot** and press **<Enter>**.
11. At the UNIXWare Login prompt, login as **root** to verify the correct setting of the password.
12. Repeat for all remaining MP and FEP machines.
13. Restart the CRS system.

CRS Password Change Day Policy

Effectively immediately, in compliance with the new Department of Commerce (DOC) Password Policy, CRS will have a password change day each quarter. The change days will be February 15, May 15, August 15, and November 15. To allow for scheduling of appropriate staff needed to make the changes and to allow for potentially life-threatening weather situations, each Weather Forecast Office (WFO) will implement the password changes within 2 weeks of the password change day. The first password change day will be May 15, 2003. Please change ALL passwords on ALL accounts on all MPs, FEPs, the VIP, and the LAN server. The DOC security policy requires that a different password be used for each account. However, it is permitted to retain the same passwords for the same accounts on different processors, e.g., the CRS user password is the same on both 0MP and 5MP.

CRS is compliant with some of the 13 password requirements described below. Other requirements will have to wait for future software builds for full compliance; still others make no sense for im plementation in CRS. For the purposes of the change day policy, sites must ensure compliance with requirements 1, 4, 8, and 9 described below. The Meteorologist in Charge (MIC) at each office will designate a staff member to be responsible for enforcing the four requirements. Requirements 1, 8, and 9 are self-explanatory; for the purposes of CRS, requirement 4 means that userid/password information for the CRS components will be maintained in a locked container in the operations area of the office that is staffed 24 hours a day, 7 days a week, so that, if necessary, the CRS Help Desk may be given the password for remote troubleshooting.

Listed below are the mandatory DOC password requirements.

Passwords must be created consistent with the following criteria:

1. Passwords must have at least eight (8) non-blank characters and comply with the following guidelines:
    a. At least one of the characters must be from the alphabet (uppercase or lowercase).
    b. At least one of the characters must be a number (0-9) or a special character (e.g., ~, !, $, %, ^, and *). [See Caution note under “General” on page A-1 of attachment A regarding the use of special characters in CRS passwords.]
    c. Six of the characters may only occur once in the password (e.g.,“AAAAAAA1" is not acceptable, but “A%rmp2g3" and “A%ArmA2g3" are acceptable).
    d. Passwords must not include any of following:
        1) Vendor/manufacturer default passwords;
        2) Names (e.g., system user names, family names);
        3) Words found in dictionaries (i.e., words from any dictionary, spelled forward or backward);
        4) Addresses or birthdays, or common character sequences (e.g., 3456, ghijk, 2468).

e. Vendor-supplied default passwords, such as SYSTEM, Password, Default, USER, Demo, and TEST, must be replaced immediately upon implementation of a new system.

NOTE: With the implementation of CRS Build 10.0/VIP Build 3.1 in September 2004, the VIP operating system, Linux Red Hat 7.3, will include the password checking described above. Sites should pay close attention to the requirement to restrict the use of words from dictionaries. In fact, Linux 7.3 prevents the use of passwords based on a dictionary word. Experience shows that the best password is based on the random generation of characters. The UnixWare operating system effective with CRS Build 10.0 includes password checking as well, but is not as extensive as that in Linux Red Hat 7.3.

2. Systems or applications that have multiple passwords for different levels of access or authentication must have unique passwords for each level.

3. Passwords must be protected to prevent unauthorized use. Specifically:

   a. Passwords must not be shared except in emergency circumstances or when there is an overriding operational necessity as documented in an operating unit System Security Plan. Once shared, passwords must be changed as soon as possible.

   b. Group passwords (i.e., a single password used by a group of users) must not be used without some other mechanism that can ensure accountability (such as separate and unique network User Ids).

   c. Group passwords must not be shared outside the group of authorized users and must be changed when any individual in the group is no longer authorized. Group passwords must never be re-used.

   d. Passwords that need to be shared because of an overriding operational necessity, as well as group passwords, cannot be used to control access to other IT systems or applications on IT systems.

4. Passwords in readable form (e.g., written on paper) must be kept in a safe location and must not be stored in a location accessible to others. For example, safe locations include storage in a locked container accessible only by the user.

5. IT systems and workstations must not display or print passwords as they are entered.

6. User applications must not be enabled to retain passwords for subsequent re-use, or be configured to bypass authentication mechanisms. For example, Internet browsers must not be enabled to save passwords for re-use.

7. Passwords must not be distributed through non-encrypted electronic mail or through voicemail, nor be left on answering machines.

8. Passwords must be changed as follows:

   a. At least every 90 days;

   b. Immediately if discovered to be compromised or one suspects a password has

been compromised;

c. Immediately if discovered to be in noncompliance with this policy or upon direction from management.

9. Do not reuse a password you have used in any of the last 8 times you have changed your password, or more recently than 2 years from when you last used the password.

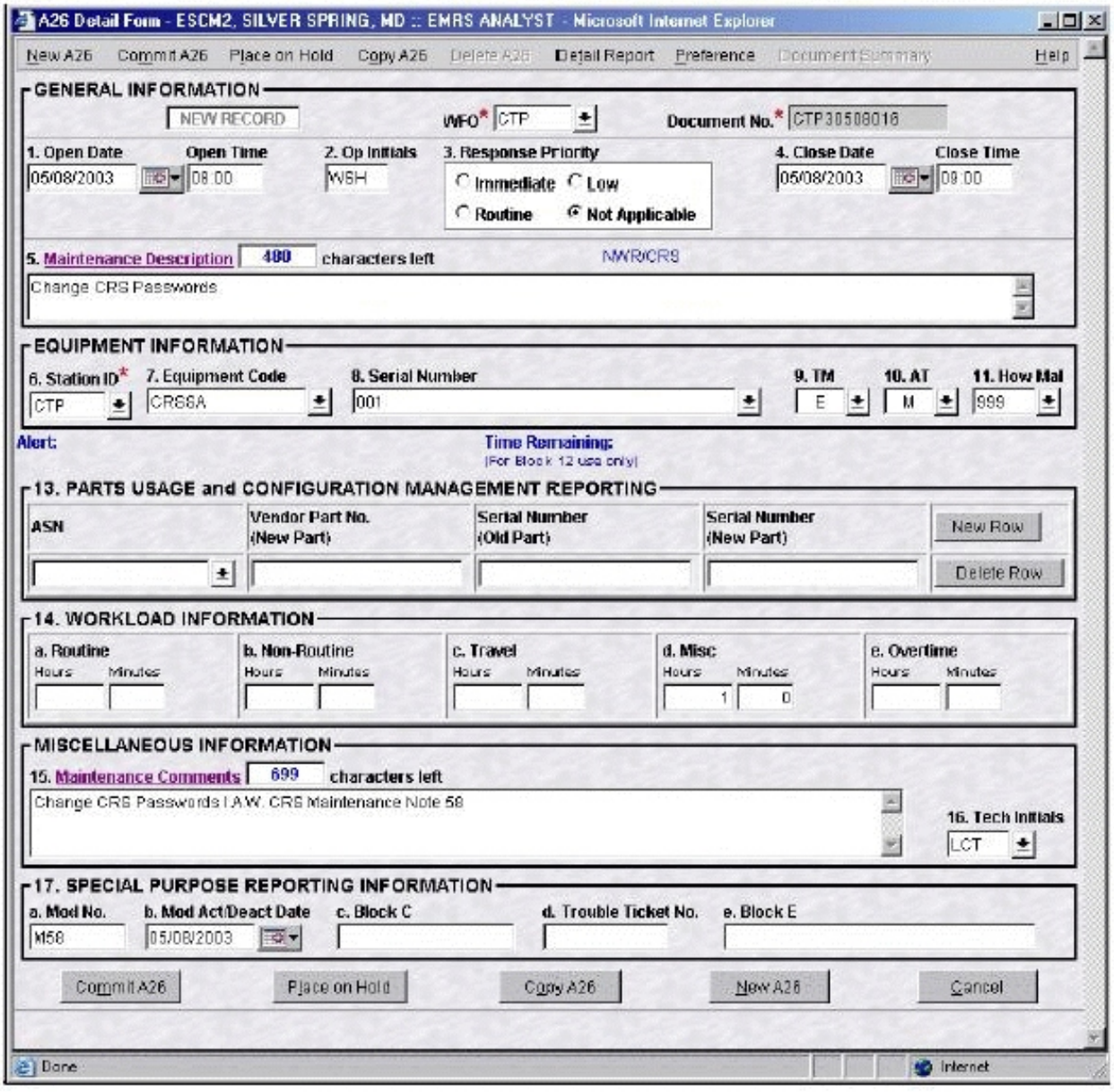
10. If a determination is made that a password has been compromised or is not in compliance with this policy, and if the password is not immediately changed, the account must be temporarily suspended until the password is changed.

11. Passwords for servers, mainframes, telecommunications devices (such as routers and switches) and devices used for IT security functions (such as firewalls, intrusion detections, and audit logging) must be encrypted when stored electronically.

12. Passwords, other than single-use (one-time) passwords, must be encrypted when transmitted across a wide area network or the Internet.

EMRS Report Sample

Initiate a maintenance report for any routine or non-routine maintenance activities associated with CRS equipment modification. Use the Engineering Management Reporting System (EMRS) Data Entry System to submit maintenance requests and to report maintenance activity. If there is no access to the data entry system, employees will follow locally established procedures to ensure proper notification of the maintenance request and documentation of maintenance activity. Detailed instructions for using EMRS are found in NWSI 30-2104.



This page left intentionally blank.